



CASE STUDY

A tight perimeter — and a live attack in progress

Manufacturing · External network pentest + OSINT

2 Critical + live threat intel

Anonymised under NDA. Client and identifying details are withheld. PXL Security LTD · Sofia, Bulgaria · pxlsec.com

CASE STUDY

A tight perimeter — and a live attack in progress

Sector	Manufacturing
Engagement	External network pentest + OSINT
Outcome	2 Critical + live threat intel

2 Critical issues	live credential-stuffing caught in progress	tight otherwise well-firewalled
-----------------------------	---	---

THE CHALLENGE

A manufacturer wanted its small, heavily-firewalled internet-facing surface and identity exposure assessed.

HOW IT UNFOLDED

1. Mapped a genuinely tight, well-firewalled perimeter.
2. Found an internet-facing remote-access gateway running an out-of-support server OS as an AD authentication boundary.
3. Confirmed it leaked internal domain and host names via an NTLM challenge.
4. Detected an active external credential-stuffing campaign in progress against several cloud-mailbox accounts.
5. Confirmed breach-corpus passwords were present but already rotated (a defensive positive); handed over provider trace IDs for log correlation.
6. Found a B2B file-transfer listener still negotiating legacy weak ciphers without mutual TLS.

KEY FINDINGS

Critical	Internet-facing remote-access gateway on an end-of-life OS
Critical	Active credential-stuffing campaign detected in progress
Medium	Internal domain/host names leaked via NTLM challenge
Medium	Legacy weak ciphers and no mutual TLS on B2B transfer

IMPACT

The company was one unpatched gateway, or one reused password, away from a foothold — and was already being probed while we tested.

OUTCOME

A prioritised remediation list (retire the end-of-life gateway, close the credential-stuffing exposure, add DMARC, mutual TLS and modern ciphers) plus actionable intelligence on an attack already underway.

TECHNIQUES

Perimeter mapping · OSINT · Credential-stuffing detection · Email security (DMARC) · Legacy TLS

SERVICES

Penetration Testing · Vulnerability Assessment



Work with PXL Security

Independent offensive-security testing since 2014 — penetration testing, red teaming and secure development, delivered by senior engineers with evidence for every finding and a retest to prove the fix.

Request a proposal: pxlsec.com/contact · hello@pxlsec.com

PXL Security LTD · 12 Vasil Levski Blvd., 1142 Sofia, Bulgaria · VAT BG203239331